

STATE of ARIZONA

Arizona Department Of Administration	Agency POLICY A800	TITLE: <u>Information Security</u> Rev. 0 Effective Date: April 30, 2007
---	--------------------------------------	---

1. AUTHORITY

The Arizona Department of Administration (ADOA) shall develop, implement and maintain a plan for information security according to related Federal (Federal Information Security Management Act of 2002, Public Law 107-347, HIPAA CFR 45 and IRS Publication 1075) and State (Government Information Technology Agency (GITA) requirements per the Arizona Revised Statutes (A.R.S.) § 41-3504(A (1)) including adopting statewide technical, coordination, and IT policy and standards (A.R.S. § 41-3504(A (1(a)))) statutes and regulations.

2. PURPOSE

To establish an ADOA information security policy for the implementation and maintenance of information security controls that will protect ADOA information resources. This policy will ensure preservation of the confidentiality, integrity and availability of information resources that is under the responsibility of the Arizona Department of Administration.

3. SCOPE

This policy applies to all ADOA Business Units, which includes divisions, contractors or other entities using agency information resources.

The ADOA Business Units, working in conjunction with the ADOA Information Security (AIS) Manager, are responsible for ensuring the effective implementation of ADOA Information Security Policies, Standards, Guidelines and Procedures .

4. DEFINITIONS

- 1. Authorized Users:** all individuals approved to use ADOA information resources and data. These include full/part-time ADOA employees, temporary employees, contract employees and non-employees providing services or products to the agency and/or non-employees who are given access to information resources, information and data (e.g. suppliers on contract or outside organizations with intergovernmental service agreements (ISAs)).
- 2. ADOA Business Units (Business Units):** all ADOA divisions, sections, work units or other entities including non-ADOA agencies, boards and commissions using ADOA information resources.
- 3. ADOA Business Unit Heads:** ADOA Agency Assistant Directors, heads of sections, work units or other entities including non ADOA agencies and persons serving as the responsible party for conducting business on behalf of ADOA.

4. **ADOA Computer Security Incident Response Team (CSIRT):** has three primary areas of responsibility: **Proactive** – coordinating implementation of preventative measures in the ADOA Business units they represent. This includes communicating about threats, new vulnerabilities, and current best practices, along with assisting IT support staff in implementing preventative measures; **Reactive** - responding to incidents in a coordinated fashion by working with technical support teams to develop the action plan and serving as the primary communication channel and technical lead for the ADOA business units they represent; **Advisory** - CSIRT members shall participate in serving as the conduit of advice between the CSIRT and the ADOA business units represented.
5. **ADOA Information Security (AIS) Manager:** is also the ADOA Senior Agency Information Security Officer and ADOA Agency HIPAA Security Officer. The AIS Manager reports to the ADOA Chief Information Officer and manages the Agency work group that develops, implements and enforces the ADOA Agency Information Security policies, standards, procedures and guidelines for the confidentiality, privacy, accessibility, availability, and integrity of ADOA Agency information resources. The AIS Manager directs the AIS group which is organized to provide information security provisioning, compliance, assessment and computer investigative support for ADOA divisions and all authorized users of ADOA information resources.
6. **ADOA Information Security Committee:** shall assess and review the security policy and standards effectiveness, impact and appropriateness. Identify alternative information security control mechanisms for the security standards as appropriate and provide for Business Unit input on Information Security issues.
7. **Configuration Management:** the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation of an automated information system, throughout the development and operational life of a system.
8. **Incident:** any event or threat of an event that affects normal ADOA information resource and/or ADOA computing facility operations. Incidents also include using ADOA information resources in connection with criminal acts or unsanctioned work.
9. **Information Asset Management:** is the creation, control, distribution, retention and final disposition of information in accordance with laws, regulations and best business practices. The goal is to ensure an open, compliant, efficient and cost effective information environment.
10. **Information Resource:** any computing device, peripheral, software, local and wide area networks (LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including the Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper,

disk space, central processor time, network bandwidth) information and data owned or controlled by the ADOA.

11. **Information Security:** the protection of information and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
12. **Information Security Control:** the management, operational, and technical safeguards or counter-measures prescribed for all ADOA information resources to protect the confidentiality, integrity, availability and accessibility of the system and its information.
13. **Software:** includes, but is not limited to, Operating Systems, utilities, database management systems, development environments, operational/management tools, business applications, communications programs, packaged personal productivity suites, etc. These can be distributed on electronic media or through electronic transmission. These can include the full products, updates, upgrades, modifications, bug fixes, maintenance releases, as well as the underlying source code.
14. **Software Development Life Cycle (SDLC):** the process of developing information systems through requirements definition, analysis, design, implementation and maintenance and disposal.
15. **Vulnerability:** a flaw in a product that makes it infeasible – even when using the product properly—to prevent an attacker from usurping privileges on the user's system, regulating its operation, compromising data on it, or assuming un-granted trust.

5. RESPONSIBILITIES

Adherence to this policy and related standards, guidelines and procedures it encompasses is the responsibility of the following people, groups or entities.

Authorized Users of ADOA Information Resources:

1. Are responsible for complying fully with all applicable Federal, State and local laws, codes, rules, regulations, and policies.
2. Shall understand that access to any ADOA information resources constitutes their acknowledgement and acceptance of all ADOA and Statewide policies, standards, guidelines and procedures , as well as software license agreements for software products used.
3. Shall understand that their use of ADOA information resources has no expectation of privacy in the use of these resources or any content therein.
4. Are responsible for following the restrictions on use of any ADOA information resource accessed or interfaced with. This can include outside software license restrictions.
5. Immediately report any known violations of this policy.

ADOA Business Unit (ADOA Business Unit Head):

1. Are responsible for ensuring that their employees fully comply with all applicable Federal and State codes, rules, regulations, and ADOA Information Security policies, standards, guidelines and procedures.
2. Shall provide assistance to the AIS Manager in monitoring the Business unit's use of ADOA information resources without prior notice or warning to any user.
3. Shall authorize the AIS Manager's requests to access the Business Units ADOA information resources at any time to ensure compliance with this policy.
4. May request to ADOA HR that an investigation of improper use of ADOA information resources be initiated.
5. Are responsible for identifying the authorized users of the Business Units ADOA information resources.
6. Shall initiate the appropriate disciplinary action to respond to violations of this policy.

ADOA Human Resources

1. Are responsible for authorizing AIS to initiate an investigation of improper use of ADOA information resources.
2. Are responsible for performing the appropriate disciplinary action to respond to violations of this policy.

ADOA Information Security (AIS) Manager:

1. Shall develop, implement and enforce the ADOA Information Security policies, standards, procedures and guidelines for the confidentiality, privacy, accessibility, availability, and integrity of ADOA information resources.
2. Shall advise ADOA Business Units on implementing their internal security-related controls.
3. Shall facilitate technical security compliance reviews for the management, configuration, and use of ADOA information resources.
4. Shall communicate with ADOA Business Unit Heads to ensure compliance with ADOA security policies, standards, guidelines and procedures.
5. Shall initiate investigations involving ADOA information resources on behalf of the ADOA Human Resources Division Assistant Director.
6. Shall manage the ADOA incident notification and ADOA Computer Security Incident Response process.
7. Shall develop, implement and facilitate the ADOA security training program.
8. Shall review and update this policy on an annual basis.

6. POLICY

ADOA Business Units shall securely protect their information resources from unauthorized and/or inappropriate access, use, disclosure, disruption, modification, or destruction. This includes all connections, public and private, internal and external to ADOA's network and information/data shared between ADOA Business Units. ADOA Business Units will comply with the legal requirements established by existing U.S. and

State statutes, this policy and its related standards, guidelines and procedures pertaining to the confidentiality, privacy, accessibility, availability, and integrity of ADOA information resources. ADOA Business Units shall be responsible for responding to all recommendations for mitigating identified risks and vulnerabilities. The Director of ADOA will be the final authority for determining the level of risk to be accepted. This policy applies to all authorized users and those who conduct business on behalf of ADOA.

6.1. MANAGEMENT SAFEGUARDS

M1 Information Security Program

An ADOA Information Security Program will be developed, implemented and administered by the ADOA Information Security (AIS) Manager with participation from all ADOA Business Units. The program shall oversee ADOA's compliance with U.S. and State, laws, codes, rules, regulations, and enforce ADOA policies, standards, guidelines and procedures regarding the secure protection of ADOA information resources. The AIS Manager will convene an ADOA Information Security Committee consisting of representatives from Business Units to participate in the implementation of required Information Security Standards. Program performance will be measured through Business Units compliance with this policy and its related standards.

M2 Risk Assessment

The AIS Manager shall conduct information risk assessments and employ risk management methods on information resources managed by the ADOA Business Units. The assessments will be used to identify the risk associated with the unauthorized access, use, disclosure, disruption, modification, or destruction of information resources. These risk assessments shall be performed according to an annual schedule or as significant changes are made to ADOA information resources. An independent information risk assessment shall be performed every three years. Business Units will be required to perform data classification and system categorization of their ADOA information resources.

M3 Security Planning

The AIS Manager will work with ADOA Business units to develop and implement security plans including a data classification, system categorization, acceptable use and privacy impact assessments for their ADOA information resources. Business Units will review their plans and make appropriate updates to reflect changes or problems identified during plan implementation or from information risk/security assessments.

M4 Acquisition, Implementation, Maintenance and Disposal

ADOA Business Units shall follow acquisition, implementation, software copyright and licensing, maintenance and disposal control methods as part of

the security planning process, to protect ADOA information resources. Disposal of ADOA information storage devices and/or media identified by divisions as surplus shall be controlled to assure secured destruction and the proper recycling so as not to harm the environment.

Initiation of, or improvements to, ADOA information resources shall include the use of system development life cycle (SDLC) methodology. This SDLC shall include security requirements and/or specifications based on assessment of risk.

M5 Security Assessments, Plans for Remedial Action and Continuous Monitoring

Periodically, ADOA Information Security (AIS) will perform security assessments to reassess the Business Unit's security controls currently in place to determine whether the current controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements (per the data classification and system categorization) of the Business Units ADOA information Resources. If a security control is found to be inadequate creating a significant vulnerability, the Business Unit shall develop a plan of action to improve the security controls to eliminate or reduce the identified vulnerabilities.

AIS will perform continuous monitoring of critical ADOA information Resources to include security impact analysis of changes to the system and ongoing assessment of security controls and status reporting.

6.2. OPERATIONAL SAFEGUARDS

O1 Personnel Security

All ADOA Business Units are responsible for employing personnel security controls that:

1. screen individuals requiring access to the ADOA's information resources, information and data prior to authorizing access;
2. terminate or modify authorized user's access upon change of employment or contract status;
3. review and update authorized access lists;
4. conduct exit interviews upon change of employment or contract status;
5. ensure the return of all ADOA information resources, information, data and access control devices; and
6. ensure that all official records created by the authorized user are stored, protected, accessible and archived per State records retention schedule and policy.
7. enforce ADOA information standards for acceptable use of ADOA information resources.

The AIS Manager will work with the ADOA Business Units to establish personnel security requirements for third party providers. The ADOA Business

Units will monitor their third party provider compliance to those requirements. The personnel security requirements will establish a formal disciplinary process for the third party provider's failure to comply with this policy and its related standards.

O2 Physical and Environmental Protection

ADOA Business Units are responsible for employing security control methods for physical and environmental protection of their ADOA information resources in compliance with ADOA Information Security Standards, Guidelines and Procedures.

O3 Contingency Planning

ADOA Business Units are responsible for employing business contingency planning methods. This will include a business contingency plan, a method for dissemination and periodic reviewing, testing and updating of their plans as appropriate.

O4 Configuration Management

ADOA Business Units are responsible for employing configuration management methods. This will include: documentation and maintenance of a current baseline configuration; controlled changes through properly authorized approvals; the monitoring and performance of security impact analysis on impact of changes and the ongoing review of current configuration settings to provide only essential capabilities and prohibit use as appropriate.

O5 System Maintenance

ADOA Business Units are responsible for employing maintenance control methods that include the scheduling, performance and documentation of routine preventative and regular maintenance of ADOA information resources.

O6 Data and System Integrity

ADOA Business Units are responsible for employing data and system integrity control methods. That includes the identification, reporting to the ADOA CSIRT of the incident and correction of potential system vulnerabilities, implementation of malicious code protection, employment of intrusion detection tools and techniques protecting the Business Units ADOA information resources.

O7 Media Protection

ADOA Business Units are responsible for employing media protection methods. That includes access controls to information in printed form or digital media removed from the system, media labeling, accountability, secure storage, transport, destruction, and disposal of ADOA information resources.

O8 Information Security Awareness and Training

ADOA Business Units are responsible for ensuring that all persons using ADOA information resources will complete required security awareness and

acceptable use of ADOA information resources training prior to authorizing access to ADOA information resources. In addition, ADOA Business Units shall ensure all authorized users complete annual security awareness and acceptable use training as a requirement to maintain access to ADOA information resources. A signed acknowledgement of Acceptable Use of ADOA information resources will be obtained from each user prior to authorizing access to the resources.

O9 Incident Management

The AIS Manager will develop, implement and manage an ADOA Computer Security Incident Response Team (CSIRT) for the purpose of restoring normal ADOA computer operations as quickly as possible in the event of a computer security incident, with the least possible impact on either the business or the user. ADOA CSIRT will consist of representatives from critical IT positions within ADOA Business Units. Activities of the Incident Management process are Incident detection, classification, communication, tracking, investigation, diagnosis, resolution and recovery.

6.3. TECHNICAL SAFEGUARDS

T1 Identification and Authentication

ADOA Business Units are responsible for employing identification and authentication control methods as defined in the ADOA information security standards related to this policy. These include, uniquely identifying and authenticating users, processes or devices accessing the ADOA information resources.

T2 Access Control

ADOA Business Units are responsible for employing access control methods as defined in the ADOA information security standards related to this policy. These access control methods authenticate and confirm authorization for the access level requested and provide required audit trails of the access granted or denied to ADOA information assets. Each authorized user of ADOA information resources shall sign an acknowledgement of their responsibilities for Acceptable Use of ADOA information resources prior to gaining access to those resources.

T3 Audit and Accountability

ADOA Business Units are responsible for employing audit and accountability control methods as defined in the ADOA information security standards related to this policy, which provide system generated audit records for auditable events, retention of audit records and protection of audit records from unauthorized access, modification and deletion.

T4 System and Communications Protection

ADOA Business Units are responsible for employing systems and communications control methods as defined in the ADOA information security

standards related to this policy. These methods provide for the prevention of unauthorized and unintended information transfer via shared system information assets, as well as protection against denial of service and malicious code attacks. Industry best practices will be employed to ensure the integrity, confidentiality, and availability of ADOA information resources. A method to establish trusted communications path between users must be evaluated to ensure the protection is commensurate with the value of the information resources.

7. POLICY NON-COMPLIANCE

For non-compliance with this policy and related standards, all ADOA employees shall be subject to Human Resource progressive discipline, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.

Contractors and other entities will be held to contractual agreements.

8. ATTACHMENTS

No attachments accompany this policy.

9. APPROVAL

Approved by:



William Bell
Arizona Department of Administration
Director

4-16-07
Approval Date